09/661,876

REMARKS

Claims 1-6, 9, 10, 14-17, 20, 21, 23-24, 32-34, 51-52, 55, 56, 59-79, and 115-118 are pending. Claims 1 and 5 has been amended.

Prior Art Rejection

The examiner rejected the claims based on Fuh in view of Brown and Abobe (the examiner inaccurately spelled it Adobe). It is respectfully submitted that this is incorrect for several reasons.

Fuh Plus Brown Fails to Teach Fundamental Element of the Claimed Invention

Fuh cannot be combined with Brown to achieve the elements of the present invention, as stated in the independent claims 1 and 5. for two reasons. Brown cannot be applied to outbound communications to the Internet because Brown work is only suitable with a limited number of nodes in the file system, followed by a properly built file structure, which is only possible on single web sites that provide web resources for visitors (i.e. inbound communications). Brown requires that the resources on the web site being accessed are highly organized in a tree-like fashion to minimize grouping and search issues with minimal available resource categories and services – to help proper access management setups by proper child/parent relationship, something that is clearly not the case for all web sites across the Internet. For example, in a highly popular web site having many different types of nodes and possibly disorganized file structure, the system becomes unmanageable and the performance will down grade substantially. See Brown column 3 lines 12-62, column 4 lines 40-45 and 58-60, column 14 lines 28-40 and 52-67 and column 26 lines 28-67. For this reason, Brown would even be unsuitable for

–31–

inbound communications of the claimed invention.

A second reason why Brown cannot be applied to the outbound communications of the claimed invention is that Brown's user access list requires a query engine server to have query processing to access information in every individual web site and this is a privileged operation. It is not possible for one server to have access to all available resources/web sites in the world. There is no single central authoritative source or query processing engine, or single source of trust, that would be given such access allowing it perform such a complex privileged operation. See Brown column 3 lines 12-62, column 4 lines 40-45 and 58-60, column 14 lines 28-40 and 52-67 and column 26 lines 28-67.

<u>Fuh Cannot Be Combined With Abobe</u>

A) Claims 1 and 5 state in their respective preambles that the claimed invention is a "system for providing filtering of outbound requests <u>for access to web sites on the Internet and/or for controlling inbound requests from the Internet</u> for access to a web site of the system" (emphasis added). The examiner incorrectly combines Fuh with Abobe to teach the proxy chaining of the claimed invention in the context of the Internet security and filtering system of the claimed invention.

Abobe is completely unsuitable for wide-scale deployment on the Internet.

Abobe, in its Abstract explicitly acknowledges this:

"This document describes how proxy chaining and policy implementation can be supported in roaming systems. ... However, as noted in the security considerations section, the techniques outlined in this document are vulnerable to attack from external parties as well as susceptible to fraud perpetrated by the roaming partners themselves. As a result, such methods <u>are not suitable for wide-scale deployment on the Internet</u>."

For this reason, it would not have been obvious to someone skilled in the art to have combined Fuh and Abobe and then modified the combination to end up with the

—32—

09/661,876

claimed invention.

For the same reason, it would not have been obvious to use proxy chaining taught by Abobe with a mobile proxy system such as the combination of Fuh in view of Brown, for added security and prvacy while surfing the Internet, as claimed by the examiner.

B) It would not have been obvious to use proxy chaining taught by Abobe with a mobile proxy system such as the combination of Fuh in view of Brown for two additional reasons. First, Abobe requires that any wireless access point (through which the client accesses the network) have the same negotiation capability as the user's original home network service. In the case of a hypothetical combination of Fuh and Abobe, the user's original home network service is protected by Fuh's proxy. When a user moves to a roaming service, Abobe would require that the wireless access point have the same negotiation capability, i.e. to provide the same access management, as Fuh's proxy. The problem is this capability cannot be achieved or assumed over the Internet because there are too many router technologies that would not be compatible for all the proxies. While Abobe is limited to a few partners, the combination of Abobe and Fuh invokes a huge unlimited number of router technologies.

A second additional reason why Fuh cannot be combined with Abobe to establish proxy chaining for roaming is as follows. Abobe talks a lot about getting account information from home AA servers when the user goes into a roaming partner. If Abobe were combined with Fuh, the home AA server would not have the user's account session information because Fuh's proxy keeps that information and Fuh's proxy does not propagate that information into the AA server. As a result, the new server does not see that information and the user's active channel with the home network will not be useful

−33−

09/661,876

for the roaming network because the user active session information is not available in the AA server. As a result, the user would be terminated and would have to start from scratch and log in again even though he had already been authenticated. Accordingly, the system would not rightfully even be called a system having true roaming capabilities.

Combining Fuh and Abobe Would Not Teach the Proxy Chaining of Claimed Invention

In addition, the proxy chaining of the claimed invention and the proxy chaining of Abobe are different enough that combining Fuh and Abobe would not make the claimed invention obvious. Specifically, the claimed invention, claim 1, page 3, third paragraph, recites "a second proxy server, without the administrative module...." This limitation clearly requires that the first proxy and the second proxy servers cannot be within the same administrative domain. In contrast, however, Aboba's second proxy server is within the same administrative domain as the first proxy server.

This can be deduced from Aboba page 5, section 5.1 entitled "Policy Implementation", which discusses a scenario where "a proxy MAY also decide to reject a request that has been accepted by the home server." Note that the term "proxy" here logically refers to the second proxy server since it is discussing proxy chaining. If the second proxy server rejects a request that has been accepted by the home server, the second proxy cannot be in the home server. It must be in the local server. The first proxy server cannot be in the home server if the second proxy server is in the local server because then it would not be called "first proxy". So both proxies must be in the local server, which is within the same administrative domain, unlike the claimed invention.

In order to clarify and emphasize this distinction between claims 1 and 5 on the one hand and the prior art (particularly Abobe) on the other hand, claim 1 has been

—34—

09/661,876

amended at page 3 with respect to its introduction of the element "a second proxy server, without the administrative module and without ~~or~~ the friendly or the unfriendly lists". In addition, residual underlining and strikethroughs (typos) were removed from claims 1 and 5 that were inadvertently allowed to remain in this clause from a previous amendment. It would have been confusing to have designated these deletions in the actual text of the claims.

Claims 2 and 6

The examiner, in item 9, contended that Fuh in view of Brown in further view of Abobe discloses the limitation of "the second proxy server has all the characteristics of a first proxy server but has an empty unfriendly outbound list" because Abobe teaches that some of the proxy servers will not have all of the accounting data. Applicant disagrees that the combination of Fuh, Brown and Abobe can be said to teach this limitation. Abobe is talking about accounting information, which is dynamic and changing. For example, the number of minutes that the user uses the system and the total charge are ever-changing. In contrast, the empty unfriendly outbound list is pre-configured and is not dynamic, constantly changing information. The examiner is therefore comparing policy information with accounting information. Thus, combining the references would not have taught this limitation of the claimed invention, as per claims 2 and 6, which refers to pre-configured policy information.

Fuh and Abobe Are Not Obvious to Combine

Fuh's transparent proxies would not be expected to be combined with Abobe's targeted proxies. Fuh (see column 2 lines 55-60) teaches away from a targeted proxy and rather teaches a transparent proxy when it states "allowing users to use remote access via

—35—

the Internet without requiring advance knowledge of the IP address of the firewall router

and without restricting to a particular host". Thus Fuh's router is a transparent proxy –

user computers are not configured to use it. One of the advantages of the client being

configured for the proxy is that the claimed invention is applicable to mesh networks

whereas Fuh's is not. In a mesh network, (it is noted that the whole world is a mesh

network including wireless services) a client might find a different router to reach the

destination and Fuh's device will fail to operate because it utilizes a transparent proxy. In

the claimed invention, in contrast, the client is configured to go to the network through

the proxy server so a centralized access control can be enforced.

For the reasons stated in the Amendment of May 5, 2008, Fuh alone does not

teach the present invention. Several reasons are reproduced here.

Fuh lacks account customization with respect to client identity and only can filter

out client requests based on using one particular pre-compiled access list called "The

Standard Access ACL". Fuh uses a single "Standard Access List" for all incoming client

requests that is not configured per user account (it is the same for all user accounts). See

Fuh col. 11, lines 28-36; col. 10, lines 28-32; col. 10 lines 49-55 and FIG. 7A, block 706.

In contrast, independent claims 1 and 5 recite the "the friendly outbound list, the

unfriendly outbound list, the friendly inbound list and the unfriendly inbound lists being

uniquely configurable for each user account".

Second, Fuh's design does not support distributed access authorization such as

protecting access to resources with multiple child de-referenced resources (such as html

pages that contain other references to resources) such as images, script files and objects,

each located on different networks.

Third, Fuh's system introduces security risks such as Trojan Horses and non-support of networks using NAT firewalls. Fuh's system does not re-authenticate the user after opening the passageway and during the active sessions. Therefore, Fuh cannot support concurrent multiple user account access authorization from a single client or from multiple clients behind firewalls implementing Network Address Translation (NAT).

The claimed invention also is distinguishable over Fuh because unlike the claimed invention Fuh cannot enforce a centralized access control system for distributed resources such as a single web page (HTML page) which behaves like a parent resource and rerouts (de-references) other resources across the network such as the programming objects attached on exhibit A. In the claimed invention the client always goes to the proxy. In Fuh, the client does not need to go to the transparent router unless it is placed between client and resource. The only way Fuh can enforce that the client goes to the router is by putting the proxy between the client network and the Internet. If the client is within the Internet and the part of the distributed resource is protected within Fuh's private network, then the client will grab the rest of the distributed resource from the Internet directly without being subject to control by Fuh's device.

Also, Fuh cannot operate in a mesh network to enforce centralized access control, as noted since a client might find a different router to reach the destination and Fuh's device will fail to operate. As noted, in the claimed invention, in contrast, the client is configured to go to the network through that proxy server so a centralized access control can be enforced.

Furthermore, the claimed invention has a further advantage over Fuh. As can be seen from Table 2 of Fuh, Fuh has a list that is nondeterministic and unstable. That is,

-37-

Fuh has approved and non-approved (denied) in the same list. The result will be different depending upon the order of how you parse through the list and aggregate the results for enforcing access rules. This was demonstrated in the May 2008 Amendment.

Since the independent claims 1 and 5 are distinguishable over Fuh, the dependent claims 2-4, 6, 9, 10, 14-17, 20, 21, 23-24, 32-34, 51-52, 55, 56, 59-79, and 115-118 are necessarily also distinguishable over Fuh.

Fuh does not disclose a first proxy server programmed to check the identity of a user ... prior to checking the identity of the requesting client ....

The claimed invention of claim 59 is distinguishable over Fuh because the claim 1 states that "the friendly inbound list and the unfriendly inbound lists being uniquely configurable for each user account". This is not the case in Fuh because Fuh's inbound list is not customizable for user accounts. The reason is the claimed invention (claim 59) authenticates the user and then authenticates the client (browser) whereas Fuh authenticates the client and then authenticates the user, as can be seen from Fuh's FIG. 7A and FIG. 7B. A client may have many users. Accordingly, when Fuh's proxy reaches the authentication of the client it does not know the identity of the user and cannot know which user list to use since he has not authenticated the user yet. Therefore Fuh cannot use a customizable inbound list. The claimed invention (claim 59) uses user account's inbound list to authenticate the client based on the user's identity. Fuh cannot do this.

Furthermore, unlike the present invention as defined by claim 59, Fuh would be subject to a Trojan Horse attack because once the legitimate user logs in and the pathway is open with no further user authentication, during the period of valid user session the Trojan horse can use the opened channel without any additional user authentication and

–38–

09/661,876

the Trojan horse can get the same resources. Under claims 59-61, 68-70. 74-76, 77-79,

however, "the first proxy server is programmed to check the identity of a user who logs

into the first proxy server" each time the user makes a request for a resource. The

differences are also evidence from a review of Fuh FIG. 7A, 7B showing data flow

diagrams.

Unlike the present invention, Fuh authenticates the client before authenticating

the user. This is seen from Fuh FIGS. 7A and 7B. In fact, Fuh cannot find the user

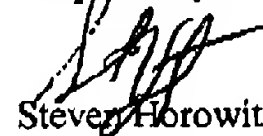authentication cache unless it knows the client IP address.

Fuh does not teach re-routing. The claimed invention, claims 68 and 71 do teach

this. See also specification page 9, 2nd para. From top, page 10, page 18.

Since all of the foregoing amendments are understood to place the application in

condition for allowance, their entry is submitted to be appropriate and is respectfully

requested. It is respectfully submitted that claims 1-6, 9, 10, 14-17, 20, 21, 23-24, 32-34,

51-52, 55, 56, 59-79, and 115-118 are in condition for allowance and it is requested that

they be allowed.

A payment of $245 is enclosed by credit card authorization form for a response

within the second month

Dated: December 18, 2008   Respectfully submitted,

                                             Steven Horowitz, Attorney for Applicant
                                             Registration No. 31,768
                                             295 Madison Avenue, Suite 700
                                             New York, NY 10017
                                             (212) 867-6800
                                             (212) 685-6862 fax
                                             sh@patentny.com

–39–